

FISH & RICHARDSON P.C.

1425 K STREET, N.W.
11TH FLOOR
WASHINGTON, DC 20005

Telephone
202 783-5070

Facsimile
202 783-2331

Web Site
www.fr.com

Date June 5, 2003

To Examiner Nobahar

Telephone: 703-305-8074



Facsimile number 06975-04100001 / 703-746-7238

From Kevin E. Greene
Technology Specialist
202-626-6376

Re Secure Data Exchange Between Data Processing Systems
Serial No.: 09/323,415
Our Ref.: 06975-041001

Number of pages
including this page 7

Message Per our telephone conversation today, our proposed claim amendments for your review.

NOTE: This facsimile is intended for the addressee only and may contain privileged or confidential information. If you have received this facsimile in error, please immediately call us collect at 202 783-5070 to arrange for its return. Thank you.

Attorney's Docket No.: 06975-04100 / Security 01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Larry T. HARADA et al. Art Unit : 2131
Serial No. : 09/323,415 Examiner : A. Nobahar
Filed : June 1, 1999
Title : SECURE DATA EXCHANGE BETWEEN DATA PROCESSING SYSTEMS

BOX AF
Commissioner for Patents
Washington, D.C. 20231

PROPOSED CLAIM AMENDMENTS FOR INTERVIEW PURPOSES

We would like to discuss the cited art as it relates to the following two proposed amendments.

Proposed Amendments 1:

1 (and 22). A data transfer method performed at a proxy server, the method comprising:
intercepting a data request from a client computer that is directed to a target server;
encrypting profile information;
~~augmenting the data request by adding~~ appending the encrypted profile information to the
data request as originally intercepted to create an augmented data request; and
sending the augmented data request to the target server.

13 (and 25). A data transfer method performed at an information server, the method comprising:
receiving an augmented data request, wherein the augmented data request includes
~~including~~ encrypted user profile information added ~~appended to a data request as originally~~
intercepted by a proxy server;
extracting the encrypted user profile information added to the data request by the proxy
server;
using the extracted profile information to generate a response; and
sending the response to the proxy server.

28. A proxy server comprising:
a database comprising records storing user profile information;

Applicant : Larry T. HARADA et al.
Serial No. : 09/323,415
Filed : June 1, 1999
Page : 2

Attorney's Docket No.: 06975-041001 / Security 01

a network interface operatively coupled to a network to exchange data with a client computer and with a target server; and

a processor operatively coupled to the network interface, the database, and a memory comprising executable instructions for causing the processor to intercept a data request that is directed to a target server, retrieve a record from the database, encrypt profile information in the record, append the encrypted profile information to the data request as originally intercepted to create an augmented data request~~augment the data request by adding the encrypted profile information~~, and send the augmented data request to the target server.

31. An information server comprising:

a network interface operatively coupling the information server to a ~~target proxy~~ server;
and

a processor operatively coupled to the network interface and to a memory comprising executable instructions for causing the processor to:

receive an augmented data request from the proxy server, wherein the augmented data request includes encrypted user profile information appended to a data request as originally intercepted by the proxy server,

decrypt the encrypted user profile information added to the data request by the target server; and

use the decrypted user profile information to generate a response to the augmented data request.

33. A method performed at a proxy server, the method comprising:

receiving a request from a client;

determining destination information associated with the request;

determining that a target server associated with the destination information should receive user profile information;

encrypting user profile information;

Applicant : Larry T. HARADA et al.
Serial No. : 09/323,415
Filed : June 1, 1999
Page : 3

Attorney's Docket No.: 06975-041011 / Security 01

appending the encrypted profile information to the data request as originally intercepted
to create an augmented data request~~augmenting the request by adding encrypted user profile~~
~~information;~~ and
sending the augmented request to the target server.

38. A system comprising:

a proxy server to:

receive a request from a client;

determine a destination information associated with the request;

determine that a target server associated with the destination information should receive
user profile information; ~~and~~

encrypting user profile information;

appending the encrypted profile information to the data request as originally intercepted
to create an augmented data request~~augment the request by adding encrypted user profile~~
~~information;~~ and

to send the augmented request to the target server.

Applicant : Larry T. HARADA et al.
Serial No. : 09/323,415
Filed : June 1, 1999
Page : 4

Attorney's Docket No.: 06975-041001 / Security 01

Proposed Amendments 2:

1 (and 22). A data transfer method performed at a proxy server, the method comprising:
intercepting a data request from a client computer that is directed to a target server;
encrypting profile information to create encrypted profile information, wherein the encrypted profile information is encrypted in a manner that allows the target server to obtain access to the profile information by decrypting the encrypted profile information;
augmenting the data request by adding the encrypted profile information to the data request; and

sending the augmented data request to the target server such that the target server can decrypt the encrypted profile information and use the profile information to generate a response to the data request.

13 (and 25). A data transfer method performed at an information server, the method comprising:

receiving an augmented data request including encrypted user profile information added by a proxy server; wherein the encrypted profile information is encrypted in a manner that allows the information server to obtain access to the profile information by decrypting the encrypted profile information

~~extracting-decrypting~~ the encrypted user profile information added to the data request by the proxy server;

using the extracted profile information to generate a response; and
sending the response to the proxy server.

28. A proxy server comprising:

a database comprising records storing user profile information;

a network interface operatively coupled to a network to exchange data with a client computer and with a target server; and

a processor operatively coupled to the network interface, the database, and a memory comprising executable instructions for causing the processor to intercept a data request that is directed to a target server, retrieve a record from the database, encrypt profile information in the

Applicant : Larry T. HARADA et al.
Serial No. : 09/323,415
Filed : June 1, 1999
Page : 5

Attorney's Docket No.: 06975-041001 / Security 01

record to create encrypted profile information, wherein the encrypted profile information is encrypted in a manner that allows the target server to obtain access to the profile information by decrypting the encrypted profile information, augment the data request by adding the encrypted profile information, and send the augmented data request to the target server such that the target server can decrypt the encrypted profile information and use the profile information to generate a response to the data request.

31. An information server comprising:

a network interface operatively coupling the information server to a target server; and

a processor operatively coupled to the network interface and to a memory comprising

executable instructions for causing the processor to:

-receive a data request from the proxy server that includes encrypted user profile information, wherein the encrypted profile information was added to the data request by the proxy server and is encrypted in a manner that allows the information server to obtain access to the profile information by decrypting the encrypted profile information,

decrypt the encrypted user profile information added to the data request by the ~~target-proxy~~ server; and

use the decrypted user profile information to generate a response to the data request.

33. A method performed at a proxy server, the method comprising:

receiving a request from a client;

determining destination information associated with the request;

determining that a target server associated with the destination information should

receive user profile information;

encrypting profile information to create encrypted profile information, wherein the encrypted profile information is encrypted in a manner that allows the target server to obtain access to the profile information by decrypting the encrypted profile information;

augmenting the request by adding the encrypted user profile information; and

Applicant : Larry T. HARADA et al.
Serial No. : 09/323,415
Filed : June 1, 1999
Page : 6

Attorney's Docket No.: 06975-041011 / Security 01

sending the augmented request to the target server such that the target server can decrypt the encrypted profile information and use the profile information to generate a response to the data request.

38. A system comprising:

a proxy server to:

receive a request from a client;

determine a destination information associated with the request;

determine that a target server associated with information should receive user profile information; and

encrypting profile information to create encrypted profile information, where in the encrypted profile information is encrypted in a manner that allows the target server to obtain access to the profile information by decrypting the encrypted profile information;

augment the request by adding encrypted user profile information; and

to send the augmented request to the target server such that the target server can decrypt the encrypted profile information and use the profile information to generate a response to the data request.